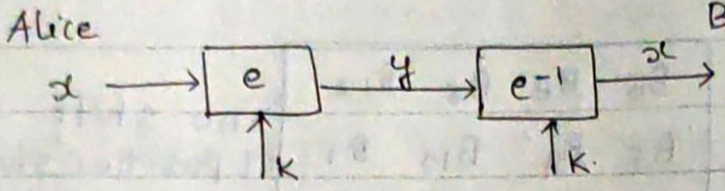
NOTES

Record the list of things you might want to do.

Chapter 5: Public Key Cryptography.

In order to understand the principle of asymmetric Cryptography let us 1st recall the basic Symmetric encryption scheme.



Such a System is Symmetric with respect to two properties.

1) Same Secret Key for encryption and decryption.
2) The encryption and decryption function are very similar

Modern day Symmetric algorithms such as AES or 3DES are very secure, fast and widespread in use. However, there are several shortcomings.

Key distribution problem:- The Key must be established between Alice and Bob using a secure channel.

Number of Keys:- Even if we solve the Key distribution problem we must potentially deal with a very large number of Keys. If each pair of users needs a separate pairs of Keys in a network on n users there are $n(n-1)/2$ Key pairs.

No protection against cheating by Alice or Bob:- Alice and Bob have the same capabilities since they possess the same Key. As a consequence Symmetric Cryptography cannot be used for applications where we would like to prevent cheating.

For instance, e-commerce application it is often important to prove that Alice sent a certain message, say an online order.

If we use symmetric cryptography and Alice changes her mind later she claim Bob has falsely generated the electronic purchase order.

Preventing this is called → non repudiation → Achieved with asymmetric cryptography.

Let $a, b \in \mathbb{Z}$ with $b > 0$ Then $\exists$, a unique $q, r \in \mathbb{Z}$ such that

$$a = bq + r \quad 0 \leq r < b.$$

Example 5.1:- $a = -5$ and $b = 3$ find q and r

$$-5 = 3q + r \quad 0 \leq r \leq 3$$

$$q = \left[\frac{a}{b}\right] \qquad r = a - b\left[\frac{a}{b}\right]$$

$[\,] \leftarrow$ greatest Integer function.

$$q = -2 \Rightarrow r = 1$$

Def 5.1:- Let $p \in \mathbb{Z}$ with $p > 1$ then p is said to be a prime number if the only positive divisors of p are 1 and itself.

Def 5.2:- If $n \in \mathbb{Z}$, $n > 1$ and is not prime, then n is composite


FOOD

"It's because of food we all work, and many are there who are unable to earn a three times meal for them, so instead of wasting food try to feed others."

Euclidean algorithm:- **

Goal:- Given two numbers r_0 and r_1 we would like to find the $\gcd(r_0, r_1)$. The largest integer that divides both of them.

Example 5.2:- $r_0 = 27$ $r_1 21$

$27 = 3 \times 3 \times 3$

$21 = 3 \times 7$

∴ The $\gcd(27, 21) = 3$.

any number $n > 1$ can be expressed as prime factors.

$r_0 = 84$ $r_1 30$

$r_0 = 84 = 2 \cdot 2 \cdot 3 \cdot 7$

$r_1 = 30 = 2 \cdot 3 \cdot 5$

$\gcd(30, 84) = 2 \cdot 3 = 6$.

2	84
2	42
3	21
7	7
	1

Example 5.3:-

Let $r_0 = 973$ and $r_1 = 301$ $\gcd(973, 301)$

$973 = 301(3) + 70$

$301 = 70(4) + 21$

$70 = 21(3) + 7$

$21 = 7(3) + 0$

$\gcd(973, 301) = 7$

"Donating and sharing can bring satisfaction in your heart that yes you have done a good deed in your life."

MAR 03 2020 TUESDAY
Wk 10 (063-303)

$154 \times 3 = 462$ $154 \times 7 = 1028$ $154 \times 6 = 924$
$154 \times 3 = 62$ $154 \times ?$ $154 \times 5 = 770$

$803 - 770 = 33$

$r_0 = 803 \quad r_1 = 154$

gcd(803, 154)

$803 = 154(5) + 33$

$154 = 33(4) + 22$

$33 = 22(1) + 11$

$22 = 11(2) + 0$

$\gcd(803, 154) = 11$.

imp **Extended Euclidean algorithm:-**

Given two integers : r_0, r_1

goal:- Compute $\gcd(r_0, r_1) = r_0 s + t r_1$

$7 = 70 - 3(21)$

$= 70 - 3(301 - 4(70))$

$= 13(70) - 3(301)$

$= 13(973 - 3(301)) - 3(301)$

$= 13(973) - 42(301)$

$s = 13 \quad t = -42.$

$11 = 33 - 1(22)$

$= 33 - 1(154 - 4(33))$

$= -33 - 1(154) - 4(33)$

$= -154 + 5(33)$

$= -154 + 5(803 - 5(154))$

$= -1(154) + 5(803) - 25(154)$

$= -26(154) + 5(803)$

$s = 16 \quad t = +3$

"We as humans with education has less helping nature than animals which are always ready to help each other."

$11 = 33 - 1(22)$

$= 33 - 1[154 - 4(33)]$

$= 5(33) - 154$

$= 5[803 - 5(154)] - 154$

$= 5(803) - 25(154) - 154$

$= 5(803) - 26(154)$

$s = 5 \quad t = -26$

Recall:- Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Then $a \equiv b \bmod m$ if $m \mid a - b$

Def 5.2:- Let $a, b \in \mathbb{Z}$. A congruence of the form $ax \equiv b \bmod m$ is a linear congruence in the variable x.

Example 5.4:- $2x = 3 \bmod 4$ is a linear congruence. There are 4 possible solution $x = 0, 1, 2, 3$.

b) $2x \equiv 3 \bmod 5$

x can take the value $0, 1, 2, 3, 4$ $x = 4$ is the solution.

Then $\{\ldots, -1, 4, 9, 14, \ldots\}$

There has to be a better way

Theorem 5.1:- Let $ax \equiv b \bmod m$ be a linear congruence in one variable and let $d = \gcd(a, m)$. If $d \nmid b$ then there is a no solution in $\mathbb{Z}$

if $d \mid b$ then the congruence has exactly d incongruent solution modulo m in $\mathbb{Z}$

"God's love is same for all, it's we human that made boundaries, let's break out this useless walls and spread the message of love and peace for all."

MAR 05 2020 THURSDAY

Wk 10 (065-301)

Theorem 5.2:-

Let $ax \equiv b \bmod m$ be a linear congruence and $d = \gcd(a,m)$. If $d \mid b$ then incongruent solution are given by $x_0 + (m/d)n$ $n = 0, 1, 2, \ldots, d-1$ where x_0 is any solution of the congruence.

Example 5.5:- $16x \equiv 8 \bmod 28$.

$d = \gcd(16, 28)$

$28 = 16(1) + 12$

$16 = 12(1) + 4$

$12 = 4(3) + 0$

$\gcd(16, 28) = 4$

$4 \mid 8$

$4 = 16 - 12(1)$

$= 16 - (28 - 16)$

$4 = 2(16) - 1(28)$

$16x \equiv 8 \bmod 28$

$28 \mid 16x - 8$.

$16x - 8 = 28y$ [a|b if $\exists c \in \mathbb{Z}$ such that $b = ac$]

$16x - 28y = 8$

$16(2) - 28(1) = 4$.

$16(4) - 28(2) = 8$

$x = 4$

$4 + (m/d)n$, $n = 0, 1, 2, \ldots d-1$

$4 + (28/4)n$, $n = 0, 1, 2, 3$

$4 + 7n$, $n = 0, 1, 2, 3$

$4, 11, 18, 25$

"Let every form of life live in his natural state, never try to hold lives in your hands, let the beauty fly."

(2) $5x \equiv 1 \bmod 16$.

$d = \gcd(5, 16)$.

$16 = 5(3) + 1$,

$5 = 5(1) + 0$.

$\gcd(5, 16) = 1$.

$1 \mid 1$.

$1 = 16 - 5(3)$ $\quad s = 1 \quad t = 3$.

$= -16$.

~~$16x \equiv$~~ $5x \equiv 1 \bmod 16$.

$16 \mid 5x - 1$

$5x - 1 = 16y$.

$5x - 16y = 1$

$5(-3) - 16(-1) = 1$

$x = -3 \quad y = 1$.

$-3 + (m/d)n$

$-3 + (16/-3)$, ~~$m = -3$~~ $0, -1, -2, -3, 0, 2, 3$

The above step is no need since we have solution as 1.

Recall → $a \cdot a^{-1} \equiv 1 \bmod m$.

Def 5.2:- Any solution of the linear congruence $ax \equiv 1 \bmod m$ is said to be a multiplicative inverse of a modulo m.

$12^{-1} \bmod 67$

$12x \equiv 1 \bmod 67$

~~xxxx~~

"Wastage is the most bad habit which normally we all have, let's take the promise not to waste food and any other eatables and better donate it so that others can taste it."

APRIL

MAR
07
2020
SATURDAY
Wk 10 (067-299)

	M	T	W	T	F	S	S
5						1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28	29	

Wk FEBRUARY 2020

$\frac{12 \times 5}{0}$

$d = gcd(12, 67)$

$67 = 12(5) + 7$

$12 = 7(1) + 5$

$7 = 5(1) + 2$

$5 = 2(2) + 1$

$2 = 2(1) + 0$

$gcd(12, 67) = 1$

$1 = 5 - 2(2)$

$= 5 - 2[7 - 5(1)]$

$= 5 - 2(7) + 5(2)$

$= (3)5 - (2)7$

$= 3(12 - 7) - (2)7$

$= 3(12) - (3)7 - (2)7$

$= (3)12 - (5)7$

$= (3)(12) - (5)[67 - (5)12]$

$= (3)12 - (5)67 - (25)12$

$1 = (28)12 - (5)67$

$12x \equiv 1 \bmod 67$

$67 \mid 12x - 1$

$12x - 1 = 67y$

$12x - 67y = 1$

$x = 28 \quad y = 5$

12×28

"Feel the beauty of blossoming flowers on branches, do not pluck them for fun or to play with, let them attached to their origin."

Euler's Phi function:-

Def 5.3:- The number of integers in Z_m relatively prime (gcd is 1) to m is denoted by $\phi(m)$.

Example 5.7:-

$m = 6$, $Z_6 = \{0,1,2,3,4,5\}$

$\phi(6) = 2$ $\quad gcd(1,6) = gcd(5,6) = 1$

No. of sets which hav gcd = 1.

$m = 5$, $Z_5 = \{0,1,2,3,4\}$

$\phi(5) = 4$ $\quad gcd(1,5) = gcd(2,5) = gcd(3,5) = gcd(4,5) = 1$

For large number we must use the following.

Theorem 5.4:- Let m have the following factorisation

$m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ where p_i are distinc Primes and $a_1, \ldots a_n$ are Positive Integers

$$\phi(m) = \prod_{i=1}^{n} (p_i^{a_i} - p_i^{a_i - 1})$$

Example 5.8:- $m = 240$

$240 = 16 \cdot 15$

$= 2^4 \cdot 3 \cdot 5$

$\phi(240) = \prod_{i=1}^{3} (2^4 - 2^3) \cdot (3^1 \cdot 3^0) \cdot (5^1 \cdot 5^0)$

$= 64$

(There are total of 64 prime number in the set)

"Let your kids be close to their grandparents, coz the working people have less time for the old, the kids at home can give company so that they can forget lonliness."

MAR 09 2020 MONDAY Wk 11 (069-297)

~~32 × 33~~ 226/~~33~~

$\frac{226}{33}$ $\frac{226}{37}$

$b = \phi = 226 = 2 \cdot 113$.

$= 2^1 \cdot 113$

$= (2^1 - 2^0)(113^1 - 113^0)$

$= (2-1)(113-1)$

$= (1)(112)$

$= 112$.

Theorem 5.5:- Let a be an integer and p a prime number and $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$ or $a^p \equiv a \bmod p$.

Example 5.9:- let $p = 7$, $a = 2$

$2^7 \equiv 2 \bmod 7$ or $2^6 \equiv 1 \bmod 7$.

$2^{89} \bmod 7$

$(2^6)^{10} \cdot 2^{29}$

$(2^6)^4 \cdot 2^5$

Theorem 5.6:- Let a and m, be integers with $\gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \bmod m$.

Principles of asymmetric cryptography.

In order to overcome the drawbacks of Symmetric key cryptography. Diffie Hellman and Merkle had a revolutionary proposal based on the following idea:- This is not necessary that the key possessed by the person who encrypts the message is secret.

"Love to hold the hands of older people and walk with them who had raised them lovingly and had taken care of you like little flowers." mom, dad

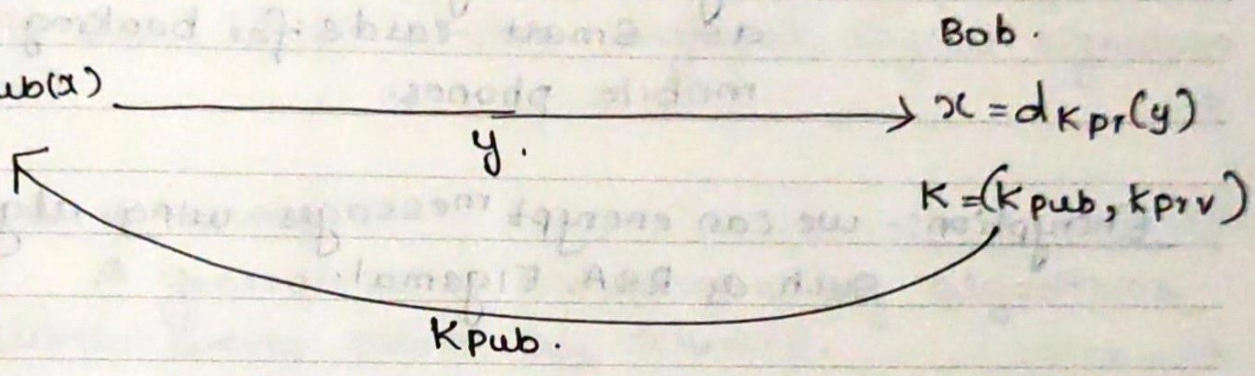
FEBRUARY 2020

Wk	M	T	W	T	F	S	S
5						1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28	29	

The crucial part is that Bob the receiver can only decrypt using a secret key.

Bob publishes a public key encryption key which is known to everyone.

Bob also has a matching secret key used for decryption. Thus Bob has two keys K_{pub}, $K_{private}$.



Recall Symmetric cryptography requires secure channel to share the key.

- There are various encryption and decryption functions.
- PK-schemes can be used for encryption of data. It turns out that we can do many other previously unimaginable things with public-key cryptography.

Key Establishment:- There are protocols for establishing ~~the~~ keys secret keys over an insecure channel.

Examples are Diffie Hellman key Exchange RSA key transport protocols.

"Little savings today can turn into big savings one day, so start saving today for a better future."

Non repudiation:- Providing nonrepudiation and message integrity can be realised with digital signature algorithms.

Identification:- We can identify entities using challenge and response protocols with digital signature e.g., in applications such as smart cards for banking or for mobile phones.

Encryption:- we can encrypt messages using algorithms such as RSA, Elgamal.

We've seen that a major advantage of asymmetric schemes is that we can freely distribute public keys. However, in practise things are a bit more tricky because we still have to assure authenticity of public keys.
In practise, this issue is often solved by certificates. Certificates bind a public key to a certain individual.

There are only three major families of public key algorithms which are of practical relevance:-

"Spare some time and money to help the needy, coz these people like us are also children of god and its our duty to help our brothers and sisters."

Integer – Factorisation schemes :-

Several PKs are based on the fact that it is difficult to factor large integers (RSA).

Discrete logarithm schemes:-

There are several log algorithms which are based on what is known as discrete log problems (DLP) in finite series (Diffie Hellman, Elgamal, Digital signature algorithm)

Elliptic curve schemes:-

A generalisation of discrete log algorithms are elliptic curves public key schemes.
(Elliptic curve Diffie Hellman, Elliptic curve Digital Signature Algorithm).

Key lengths and Security levels:-

All 3 of the established PK-algorithm families are based on number-theorectic function. They:

→ They require arithemetic with very long operands and keys.

- Longer operands and keys the more secure the algorithm
- Inorder to compare the different algorithms one must often consider the security level.
- An algorithm is said to have a security level

"Preserve and save food from getting wasted, so that others can also taste who are not getting it."

of n bits, if the best known attack requires 2^n steps.

Algorithm	cryptosystems	Security level. 80	128	192	256
Inter fatorisation	RSA	1024 Key bit	3072	7080	15360
Discrete log.	Diffie hellmon Elgamal Digital signature algo	1024	3072	7080.	15360
Elliptic curves.	ECDH, ECDSA.	160	256	384	512
Symmetric	AES, DES	80	128	192	256.

RSA

Invented in 1977 by Ronald Rivest, Adi shamir and Leonard Adleman.

most popular Pk cryptosystem
Patented in the USA until 2000 so it was difficult for people to use

RSA algorithm:-

Key generation:- unlike symmetric algorithms (AES, 3DES) PK algorithms require the computation of the key pair (K_{pub}, K_{prv})

"We can do a good deed alone, then if we join hands we can do something great for the benefit of others."

1) choose large prime numbers p and q

2) compute $n = pq$

3) Compute $\phi(n) = (p-1)(q-1)$

4) Select public exponent $e \in \{1, 2, \cdots, \phi(n)-1\}$. Such that gcd

It is important to inverse.

5) Compute the private key d such that $de \equiv 1 \bmod \phi(n)$

public key $K_{pub}(n, e)$

$K_{pr} = d$.

RSA Encryption and Decryption.

Given $K_{pub} = (n, e)$ and message $x \in Z_n = \{0, 1, 2, \ldots, n-1\}$

6) $y = e_{K_{pub}}(x) \equiv x^e \bmod n$.

7) $K_{pr} = d$, $y \in Z_n$ $x \equiv d_{K_{pr}}(y) \equiv y^d \bmod n$.

Example 5.9!-

Alice wants to send an encrypted message to bob. Bob first computes his RSA parameters. He then sends Alice the public key. Alice encrypts the message $x = 4$ and sends Ciphertext y to Bob. Bob decrypts y using his private key. Given Bob chooses $p = 3$ and $q = 11$

1) $p = 3$ $q = 11$

2) $n = p \times q = 33$

3) $\phi(n) = (2)(10) = 20$

"We must be helpful by nature, loving by heart and pure at mind then we can sum up as complete human beings."

MAR 15 2020 SUNDAY

Wk 11 (075-291)

4) Choose exponent e such that $e \in \{1, \ldots, 19\}$ and $\gcd(e, 20) = 1$

Bob chooses $e = 3$ { no common factor between 3, 20}

5) $de \equiv 1 \bmod \phi(n)$

$3d \equiv 1 \bmod 20$

$\gcd(3, 20) = 1$

$20 = 3(6) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$1 = 3 - 2$

$= 3(1) - (20 - 3(1))$

$= 3(7) - 20$ $d = 7$

$20 \mid 3d - 1 \Rightarrow 20y = 3d - 1$

$1 \equiv 3d - 20y$

$d = 7$

Alice

$x = 4$

$y \equiv 4^3 \bmod 33$

$y = 31$

$K_{pub} = (3, 33)$ ← Bob

$y = 31$ →

$x \equiv 31^7 \bmod 33$

$x \equiv (-2)^7 \bmod 33$

$\equiv (-128) \bmod 33$

$\equiv 4$

"Helping and loving the old is the best deed you can do coz old-ones are often seem neglected in their homes."

Fast Exponentiation

Unlike symmetric algorithms such as AES, DES or stream ciphers, public key algorithms are based on arithmetic with very ~~long~~ large numbers.

problem in practise $y \equiv x^e \bmod n$, $x \equiv y^d \bmod n$ } with large numbers.

Example 5.10.

$x^4 = ?$

Naive way is $x \cdot x = x^2$

$x^2 \cdot x = x^3$

$x^3 \cdot x = x^4$

cost is 3 multiplications.

Better way

$x \cdot x = x^2$

$x^2 \cdot x^2 = x^4$

cost 2 multiplications.

x^8.

Naive way

$x \cdot x = x^2$

$x^2 \cdot x = x^3$

$x^3 \cdot x = x^4$

$x^4 \cdot x = x^5$

$x^5 \cdot x = x^6$

$x^6 \cdot x = x^7$

$x^7 \cdot x = x^8$.

cost is 7

Better way

$x \cdot x = x^2$

$x^2 \cdot x^2 = x^4$

$x^4 \cdot x^4 = x^8$

cost is 3.

$x^{2^{1024}}$

Stupid way $= x \cdot x = x^2$

$x^2 \cdot x = x^3$

$\vdots$

$x^{2^{1024}} \cdot x = x^{2^{1024}}$

} $2^{1024} - 1$ multiplications

Not enough ink in this universe for me to do such calculations.

"When we help someone to lift up, that means we are adding a good deed in our account, and someone will surely pick you up when you will fall some day."

Betterway.

$x \cdot x = x^2$

$x^2 \cdot x^2 = x^4$

$x^{2^{1022}} \cdot x^{2^{1023}} = x^{2^{1024}}$ } 1024 multiplication.

Square and multiply algorithm.
"binary method"
"left-to-right" exponential

Example 5-11:- x^{26}

$x \cdot x = x^2$ Square
$x^2 \cdot x = x^3$ Mul
$x^3 \cdot x^3 = x^6$ Square
$x^6 \cdot x^6 = x^{12}$ Square
$x^{12} \cdot x = x^{13}$ Mul
$x^{13} \cdot x^{13} = x^{26}$ Square

} 4 square 2 mul.

$x^{26} = x^{11010}$.

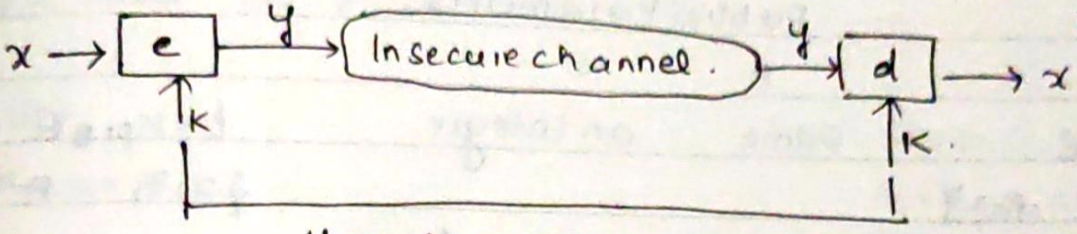
$(x^1)^2 = x^{10}$
$(x^1)^2 \cdot x = x^{11}$
$(x^{11})^2 = x^{110}$
$(x^{110})^2 = x^{1100}$
$(x^{1100}) \cdot x = x^{1101}$
$(x^{1101})^2 = x^{11010}$.

"If you are good in your actions and helpful in your mind then you will sometimes even help those who are your biggest enemies."

Discrete logarithm:-

old problem.

Alice



Have to exchange keys (This is the problem).

The Diffie-Hellman key exchange protocol proposed by whitfield Diffie and Martin Hellman in 1976 way the 1st asymmetric scheme published in open literature.

It provides a practical solution to the key distribution problem i.e., it enables two parties to derive a common secret key by communicating over an insecure channel.

Diffie-Hellman key exchange is a very impressive application of the discrete logarithm problem (DLP).

This key agreement technique is implemented in many open and commercial cryptographic protocols like:- Secure shell (SSH)
Transport Layer Security (TLS)
Internet Protocol security (IPsec)

The basic idea behind Diffie Hellman key Exchange is that Exponential in Z_p^*; P → prime is a one-way function and that exponential is commutative.

"The life is a precious gift to all by god and saving the precious life of someone means you have done something which makes you near to god."

$K = (\alpha^x)^y$

$= (\alpha^y)^x \bmod p$

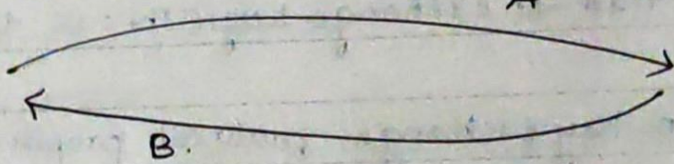
Alice | Public Parameters | Bob

p α

Prime | an integer

$a = K_{pr,A} \in \{1,2,3,\cdots,p-2\}$

$b = K_{pr,B} \in \{2,3,\cdots p-2\}$



$A = \alpha^a \bmod p$

$B = \alpha^b \bmod p$

$K_{AB} = B^a \bmod p$

$K_{AB} = A^b \bmod p$

① Choose a large prime p.

② Choose an integer $\alpha \in \{2,3,\cdots,p-2\}$

③ publish p, α

④ Alice selects $a \in \{2,3,\cdots,p-2\}$

Bob selects $b \in \{2,3,\cdots,p-2\}$

⑤ $A = \alpha^a \bmod p$, $B = \alpha^b \bmod p$ (exchange A and B)

⑥ $K_{AB} = B^a \bmod p = A^b \bmod p$

Proof:- Alice computes

$B^a \bmod p$

$(\alpha^b)^a \bmod p$

Bob computes:

$A^b \bmod p$

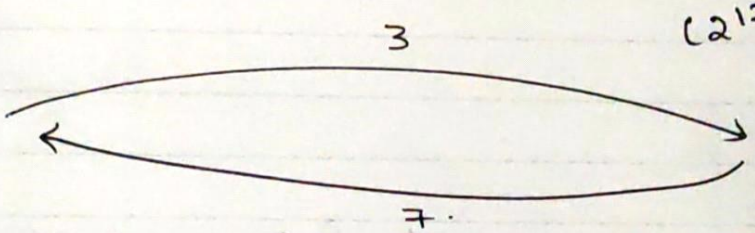
$(\alpha^a)^b \bmod p$

"Saving life of others is the best chance anyone can get to do in his lifetime."

Alice $\quad y \in AES_{K_{AB}}(x)$ $\xrightarrow{\quad y \quad}$ Bob $\quad x = AES^{-1}_{K_{AB}}(y)$

Example 5.12:- Let $P = 29$ and $\alpha = 2$

Alice	Bob
$a = k_{prA} = 5$	$b = k_{prB} = 12$
$A = 2^5 \bmod 29$ $= 3$	$B = 2^{12} \bmod 29$ $= 7$ $(2^{12} = 2^5 \cdot 2^5 \cdot 2^2$ $3 \cdot 3 \cdot 4 \bmod 29$ $36 \bmod 29 = 7)$
$K_{AB} = 7^5 \bmod 29$ $= 16$	$K_{AB} = 3^{12} \bmod 29$ $= 16$



Finite Groups.

Group ≈ "set of elements and 1 group operation". we looked at the real definition a few weeks back.

In short

In short:

1. Closeness $a \circ b = c \in G$
2. Associative $(a \circ b) \circ c = a \circ (b \circ c)$
3. Neutral element $(a \circ 1) = a$

} } do.

"Let's not think only about ourselves, we have to take care of all which are dear and near to us."

MAR 21 2020 SATURDAY

Wk 12 (081-285)

4. Inverse element $a \circ a^{-1} = 1$ } Group } Abelian group.

5. $a \circ b = b \circ a$

X	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0								
5	0								
6	0								
7	0								
8	0								

Problem: inverses only exists for $\{1, 2, 4, 5, 7, 8\}$ because $\gcd(a, a) = 1$

Define $Z_a^* = \{1, 2, 4, 5, 7, 8\}$ we throw away the one's without inverse

Theorem 5.1:- The set Z_n^* consists of all integers $i = 0, 1, 2, \ldots, n-1$ for which $\gcd(i, n) = 1$. This forms an abelian group under multiplication modulo n ($e = 1$)

↑ Identity

"See the talent in your kids and then encourge them to choose as their field in which they can master in the future."

Note:- Z_p^*, where p is prime forms a multiplicative group.

$\gcd(a,p)=1$

$Z_p^* \{1,2,\ldots,p-1\}$.

Cyclic groups:-

Def 5.3:- A group $(G,0)$ is finite if it has finite number of elements.

we denote the cardinality or order of the group G by $|G|$

3^{11}

$3^4 \cdot 3^4 \cdot 3^3$

$4 \quad 4 \cdot 5 \quad 80 \bmod 11$

3

Example 5.14:

$(Z_n, +)$

$|Z_n| = n$.

$(Z_n^*, \bullet)$.

$|Z_n^*| = \phi(n)$

$Z_7^* = 6$

$Z_8^* = 4$.

$Z_{11}^* = 10$.

Example 5.15:- $Z_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$

what happens if we compute all powers of 3?

$3^1 \equiv 3 \bmod 11$

$3^2 \equiv 9 \bmod 11$

$3^3 \equiv 5 \bmod 11$

$3^4 \equiv 4 \bmod 11$

$3^5 \equiv 1 \bmod 11$

$3^6 \equiv 3 \bmod 11$

$3^7 \equiv 9 \bmod 11$

$3^8 \equiv 5 \bmod 11$

$3^9 \equiv 4 \bmod 11$

$3^{10} \equiv 1 \bmod 11$

$3^{11} \equiv 3 \bmod 11$.

"Those who can spare time from their busy schedules to help and serve our earth, is the best work we can do in our lives."

Def 5.4:-

The order ord(a) of an element a of a group $(G, \circ)$ is the smallest ~~group~~ positive integer k such that-

$$a^k = a \circ a \circ a \circ \cdots \circ a = 1$$

where 1 is the identity element of G.

$ord(3) = 5$

We see that from this point, the powers of 3 run through $\{3, 9, 5, 4, 1\}$ indefinetly.

Def 5.5:- A cyclic group

A group G we contains an element α with the maximum order $ord(\alpha) = |G|$ which is said to be cyclic.

Elements with maximum order are called primitive elements or generator.

$a = 2$

$2^1 = 2 \bmod 11$
$2^2 = 4 \bmod 11$
$2^3 = 8 \bmod 11$
$2^4 = 5 \bmod 11$
$2^5 = 10 \bmod 11$
$2^6 = 9 \bmod 11$
$2^7 = 7 \bmod 11$
$2^8 = 3 \bmod 11$
$2^9 = 6 \bmod 11$
$2^{10} = 1 \bmod 11$

$ord(2) = 10$.
$|G| = 10$
2 is a generator of Z_{11}^*

"When you want something good to be done
then forget the rules of untouchability, caste, colour rather
remember humanity, peace and love"

cyclic groups are the basis of discrete logarithm cryptosystems.

Theorem 5.7:- For every prime P, $(Z_p^*, \cdot)$ is an abelian finite cyclic group.

Important properties

1) Let $a \in G$, G → cyclic group.
2) 1.) $a^{|G|} = 1$
   2) Ord(a) divides |G|

Example 5.17:

$Z_{11}^* = 10$.

The only element order in this group are 1, 2, 5, 10.

Ord(1) = 1	ord(6) = 10
Ord(2) = 10	ord(7) = 10
ord(3) = 5	ord(8) = 10
ord(4) = 5	ord(9) = 5
ord(5) = 5	ord(10) = 2.

How many primitive elements / Generator = 4.

Why do we care?

cyclic groups can make nice DLP.

$Z_{47}^* = \{1, \ldots, 46\}$

$\alpha = 5 \leftarrow$ generator.

$5^x = 41 \bmod 47$

hard problem in cryptography.

"Join hands for a good cause, and let others also join so that the good which you decided to do must be done at the earliest with multiple helping hands ."

MAR 25 2020 WEDNESDAY
Wk 13 (085-281)

In DH
$B = \alpha^b \bmod p$, α is known, B is known, p is known att
wants b which is hard.

Discrete log problem
Def 5.5:- Given the finite cyclic group Z_p^* of order
$p-1$ and a primitive element $\alpha \in Z_p^*$
and another element $\beta \in Z_p^*$. The
discrete log problem is the problem of
determining the integer $1 \le x \le p-1$ such that
$\alpha^x = \beta \bmod p$.

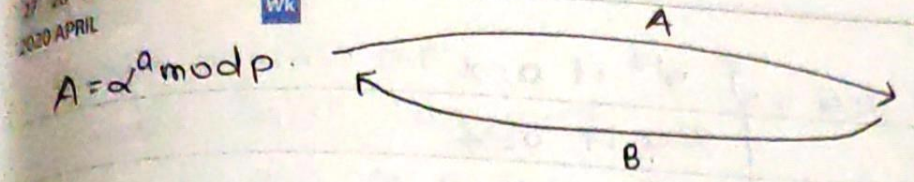
Example 5.18:-
$2^x \equiv 9 \bmod 11$
$x = 6$ by Brute force.

Example 5.19:-
$5^x \equiv 41 \bmod 47$
$x = 15$ by brute Force.

Diffie-Hellman Problem (DHP)
Recall:- DH Key Exchange.

Alice — α, p — Bob
$a = k_{pA} \in \{2 \dots p-1\}$
$b = k_{pB} \in \{2 \dots p-1\}$

"You can do three good deeds for the earth, donate the useless, recycle the waste and stop wasting food."



$K_{AB} = B^a \bmod p$ $\qquad$ $K_{AB} = A^b \bmod p$.

Security:-

Assumption: Oscar can only listen (passive)

Oscar knows α, prime p, A, B.

he wants $K_{AB} = \alpha^{ab} \bmod p$.

This is called the Diffie-Hellman problem. (DHP)

One way of solving the DHP is 1) compute $a = \log_\alpha A \bmod p$.

2) compute $B^a \bmod p = K_{AB}$.

↳ This is a very hard step.

unfortunately for Oscar step 1 is computationally a very hard problem is p is large enough.

Generalised DLP.

one powerful feature of DLP is not restricted to Z_p^* but other cyclic groups can also be used for building Discrete log cryptosystems.

Generalised DLP:- given cyclic group $(G, \circ)$ and $|G| = n$

Let α be a primitive element and $\beta \in G$ Find x such that $\beta = \alpha^x = \alpha \circ \alpha \circ \alpha \circ \ldots \circ \alpha$.

where $1 \le x \le n$

"When it comes the need for help then forget the person you are helping is your competitor rather remember he too is a human being who needs your help and support right now."

APRIL

$\beta = \alpha \circ \alpha \circ \ldots \circ \alpha = \begin{cases} \alpha^x \text{ if } \circ = \times \\ x\alpha \text{ if } \circ = + \\ x \in Z. \end{cases}$

which other cyclic groups make discrete log problem?

1) $GF(2^m)^*$ multiplicative group of extension fields.
2) Prime fields multiplicative groups.
3) Elliptic curves:- points on a curve lead to a discrete log problem.
4) hyper Elliptic curve. (Generalization of curves)

Eg:- 5.20:- Group is $G = (Z_{11}, +)$ is a finite cyclic group with $\alpha = 2$.

i	1	2	3	4	5	6	7	8	9	10	11
$i\alpha$	2	4	6	8	10	1	3	5	7	9	0

Now try to solve Discrete log problem for $\beta = 3$

we have to compute x such that $1 \le x \le 11$

$x \cdot 2 = 2 + 2 + \cdots + 2 \equiv 3 \bmod 11$

$x \equiv 2^{-1} \cdot 3 \bmod 11$ inverse of 2 is 6

$x \equiv 6 \cdot 3 \bmod 11$

$= 18 \bmod 11$

$= 7 \bmod 11$

$2x \equiv 1 \bmod 11$

$\gcd(2, 11) = 1$

$x = 6$

"Donating your belongings is a good deed but if you can put an extra effort to collect donations from others and give them to the needy it can be more than needful."

Attack against DLP:

Goal: Solve $\log_\alpha \beta = x$

$\alpha, \beta \in G$, $n = |G|$ $\alpha^x = \beta$.

$n = \log_\alpha A \bmod p$

$B^a = K_{AB} = \alpha^{ab} \bmod p$.

① Attack by Brute Force

$\alpha^1 = \beta$
$\alpha^2 = \beta$
$\vdots$
$\alpha^n = \beta$

} requires $O(n)$ steps.

if this is the only attack $n \geq 2^{80}$ to make a brute force search infeasible

Then $|G| = p-1$ should be atleast in the order of 2^{80}.

② Square-root attack:

Baby step giant step algorithm and pelland's sho method

a) compile in $\sqrt{n}$ steps

if $n \approx 2^{80}$

$\sqrt{2^{80}} = 2^{40}$

To resist these attacks must have $n \geq 2^{160}$ group elements.

Side Note: This is why elliptic curves (EC) have atleast 160 bits

Square route attack work in any group. for EC they are the best known attacks.

"Freedom is a choice for all, open the cage of birds and see the happiness through their nonstop chirping as they are thanking you for this good action."

3) Index-calculus attack

For certain groups G the more powerful index calculus attack exists in particular the attack works in Z_p^* and $GF(2^m)^*$

In practice p, $2^m \geq 1024$ often p is in range of $2^{1024} \ldots 2^{2048}$ bits.

Decimal digits	Bit length	Date.
58	193	1991
65	216	1995
85	282	1999
100	332	2000
120	391	2001
135	448	2006
160	532	2007.

Elgammal Encryption scheme.

Encryption with the DLP.

First: what can we do with PK algorithms.

Services	Integer factor	DL Z_p^*	EC
Key Exchange	RSA	Diffie Hellman	EC, Diffie Hellman (ECDH)
Digital signat	RSA	Elgammal, Digital Std, Algorithm (DSA)	ECDH

RSA Elgamal EC Elgamal

"Not only true humanity is seen among humans also sometimes animals set an example of pure hearts and helpful nature."

Goal: Develop an encryption scheme based from DH-Key exchange.

Advantages of Elgamal over direct DH-Encryption.

1)
2)
3)

Alice — Bob

α, p

$A = \alpha^a \bmod p$ ← B — $B = \alpha^b \bmod p$.

$B^a = \alpha^{ab} \bmod p$ → A → $A^b = \alpha^{ab} \bmod p$

$= K_{AB}$ $= K_{AB}$.

message x

$y \equiv x \cdot K_{AB} \bmod p$ → y → $x \equiv y \cdot K_{AB}^{-1} \bmod p$.

In order to understand the Elgammal Scheme, it is very helpful to see how it follows from DHKE

- The idea is that Alice uses the key as a multiplicative mask to encrypt x as $y = xK_{AB} \bmod p$.

"All of us smile and want to be close to happy people
but those who gave hands to pull the people who are sad, crying,
needy are the real heroes of humanity."

Elgammal Encryption Protocol:

Elgammal was invented around 1985, very similar to D_H but with reordering of steps also spelled Elgammal.

Alice		Bob.
	① $k_{pub} = (p, \alpha, \beta)$ ←	choose large prime p, and $\alpha \in Z_p^*$ $k_{pr} = d \in \{2, \dots, p-2\}$ compute k_{pub}:- $B = \alpha^d \bmod p$.
Choose $i \in \{2 \dots, p-2\}$ Computes ephemeral key $k_E = \alpha^i \bmod p$ ②		
computes making key $k_m = B^i \bmod p$ ③		
encrypts $y = x \cdot k_m \bmod p$ ④	⑤ (k_E, y) →	compute making key $k_m = k_E^d \bmod p$ ⑥ decrypt $x \equiv y \cdot k_m^{-1} \bmod p$ ⑦

Here Alice only has to send one message to Bob instead of 2

Proof: Bob computes

$$\begin{aligned} & y \cdot k_m^{-1} \bmod p \\ \equiv\ & [x \cdot k_m] \cdot (k_E^d)^{-1} \bmod p \\ \equiv\ & [x \cdot \beta^i] \cdot k_E^{-d} \bmod p. \\ \equiv\ & [x \cdot \beta^i] \cdot (\alpha^i)^{-d} \bmod p \\ \equiv\ & [x \cdot (\alpha^d)^i] \cdot (\alpha^i)^{-d} \bmod p \\ \equiv\ & x. \end{aligned}$$

"If you have taught your kids to help others when in need, that means you are on the way to make them the responsible citizens of tomorrow."

APR 01 2020 WEDNESDAY

Wk 14 (092-274)

Example 5.21: Bob generates the Elgamal keys and Alice encrypts the message $x = 26$.

Alice		Bob
$x = 26$, choose $i = 5$	$K_{pub,B} = (p, \alpha, \beta)$ ←	$p = 29$, $\alpha = 2$
$K_E = \alpha^i \bmod p$		Choose $K_{pr,B} = d = 12$
$= 2^5 \bmod 29$		Compute $\beta = \alpha^d \bmod p$
$= 3$.		$= 2^{12} \bmod 29$
		$= 7 \bmod 29$
$K_m = \beta^i \bmod 29$		
$= 7^5 \bmod 29$		
$= 16$.		
$y = x \cdot K_m \bmod p$		
$= 26 \cdot 16 \bmod 29$	$y = 10, 3$ →	$x = y \cdot K_m^{-1} \bmod p$
$= 10 \bmod 29$		$K_m = K_E^d \bmod p =$
		$= 3^{12} \bmod 29$
		$= 16$
		$x = 10 \cdot 20 \bmod 29$
		$= 26$.

$16 z \equiv 1 \bmod 29$
$z = 16^{-1} \bmod 29$
$= 20 \bmod 29$

Example 5.22

$\alpha = 2$

$d = 3$

$i = 4$

$z = 8$

$p = 11$

"One can get anything if he is willing to help enough, others get what they want, coz true happiness lies in helping others"

Alice

$x = 8$, $i = 4$

$K_E = \alpha^i \bmod p$

$= 2^4 \bmod 11$

$= 5$

$K_{pub,B}(p, \alpha, \beta)$

Bob

$p = 11, \alpha = 2$

Choose $K_{pri} = d = 3$

compute $\beta = \alpha^d \bmod p$

$= 2^3 \bmod 11$

$= 8 \bmod 11$

$K_m = \beta^i \bmod 29$

$= 8^4 \bmod 29$

$= 8^2 \cdot 8^2$

$= 4 \bmod 11$

$y = x \cdot K_m \bmod p$

$= 8 \cdot 4 \bmod 11$

$= 32 \bmod 11$

$= 10 \bmod 11$

$y = 10, 5$

$x = y \cdot K_m^{-1} \bmod p$

$K_m = K_E^d \bmod p$

$= 5^3 \bmod 11$

$= 5^2 \cdot 5 \bmod 11$

$= 15 \bmod 11$

$= 4 \bmod 11$

$4 \cdot 1 \equiv 1 \bmod 11$

$q = 4 \cdot 3 \bmod 29$

$= 12 \bmod 11$

$K_m^{-1} = 3$

$x = 10 \times 3 \bmod 11$

$30 \bmod 11$

$= 8$

"Fashion your life as a garland of beautiful deeds, not performed as any big action, but as small-small acts which can impart happiness to any form of life."

APR 03 2020 FRIDAY
Wk 14 (094-272)

$5 \equiv 1 \bmod 4$
$1 \equiv 5 \bmod 4$
$a \equiv b \bmod m$ iff $m \mid a-b$
$4 \mid 5-1$

$4 \mid 1-5$
$4 \mid -4$

Computational Aspects

Alice and Bob have to compute $\beta = \alpha^d$, $K_E = \alpha^i$ $K_m = \beta^i$ } Square and multiply

Question:- How do we compute

$K_m \equiv K_E^d \bmod p$ ← Square and Mul algorithm.

K_m^{-1} ← Extended Euclidean algorithm.

$x = y K_m^{-1}$ ← multiplication

Can merge $K_m \equiv K_E^d \bmod p$ and K_m^{-1} and apply square and multiply.

Fermat's little Theorem:- $K_E \in Z_p^*$

$K_E^{p-1} \equiv 1 \bmod p$.

$K_m^{-1} \equiv (K_E^d)^{-1} \bmod p$.

$K_m^{-1} \equiv K_E^{-d} \bmod p$.

$K_m^{-1} \equiv K_E^{-d} \cdot K_E^{p-1} \bmod p$

$K_m^{-1} \equiv K_E^{p-1-d} \bmod p$.

Attacks

Oscar does not know i or d.

(i) Compute DLP:- $d = \log_\alpha \beta$

$\Rightarrow$ Compute $K_m = K_E^d$

$x \equiv y K_m^{-1}$

or

compute $i = \log_\alpha K_E$

"Seek to do good in your life, and you will find that happiness will run after you each and every day."

$Y_1 X_1^{-1} = Y_2 X_2^{-1}$

$X_2 Y_1 X_1^{-1} = Y_2$

$X_2 Y_1 = Y_2 X_1$

$X_2 = Y_2 X_1 Y_1^{-1}$

$\Rightarrow$ Compute $K_m = B^i$

$a = y K_m^{-1}$

This is difficult to do, if the DLP is computationally hard problem (long primes) $\Rightarrow p \geq 2^{1024}$.

2) Attack Re-use of Secret exponent.

maybe software key.

$K_E \equiv \alpha^i$ $\qquad K_m \equiv B^i$

$y_1 = x_1 K_m \xrightarrow{(y_1, K_E)}$

$y_2 = x_2 K_m \xrightarrow{(y_2, K_E)}$

Oscar: the sees i is the same since K_E is the same

$\Rightarrow K_m$ is the same Assume he knows x_1

$K_m = Y_1 X_1^{-1} = Y_2 X_2^{-1}$

Solve for

$X_2 \equiv Y_2 \times Y_1^{-1} \bmod p$.

"Success means we go to sleep at night knowing that our strength and energy were used in a way that served others."